1. Wireshark
• Wireshark is one of the few open-source cybersecurity tools to offer user training. However, the GUI is limited, and you need to refer to the documentation constantly when using Wireshark.

https://www.wireshark.org/

2. OpenIAM
• OpenIAM offers automation, GUI, integrations, and self-service, despite being an open-source platform. However, the documentation may be limited, generating very few analytical reports.

https://www.openiam.com/

3. Nmap
• The tool detects and documents nearly every type of network activity through a command-line interface or GUI. However, its functionalities are limited only to network mapping, and you will need to explore the community's other tools to maximize its functionalities.

https://nmap.org/

4. Metasploit
• Metasploit is one of the most popular pen-testing frameworks in the world. However, the free version can be limited, and you may have to upgrade to Pro to access the business user interface.

https://www.metasploit.com/

5. John the Ripper
• Passwords are among the top weak links when it comes to enterprise cybersecurity and John the Ripper helps run thorough password audits. However, it requires a significant amount of technical expertise and familiarity with Unix.

https://github.com/openwall/john

6. Sooty
• Sooty is a tool developed with the task of aiding SOC analysts with automating part of their workflow. One of the goals of Sooty is to perform as many of the routine checks as possible, allowing the analyst more time to spend on deeper analysis within the same timeframe.

https://github.com/TheresAFewConors/Sooty

7. Peepdf
• peepdf is a Python tool to explore PDF files to find out if the file can be harmful or not. The aim of this tool is to provide all the necessary components that a security researcher could need in a PDF analysis without using 3 or 4 tools to make all the tasks. With peepdf it's possible to see all the objects in the document showing the suspicious elements, supports the most used filters and encodings, it can parse different versions of a file, object streams and encrypted files. With the installation of PyV8 and Pylibemu it provides Javascript and shellcode analysis wrappers too. Apart of this it is able to create new PDF files, modify existent ones and obfuscate them.

https://eternal-todo.com/tools/peepdf-pdf-analysis-tool

8. PyREBox
• PyREBox is a Python scriptable Reverse Engineering sandbox. It is based on QEMU, and its goal is to aid reverse engineering by providing dynamic analysis and debugging capabilities from a different perspective. PyREBox allows to inspect a running QEMU VM, modify its memory or registers, and to instrument its execution, by creating simple scripts in Python to automate any kind of analysis. It also offers a shell based on Python that exposes a rich set of commands, as well as a Python API.

https://talosintelligence.com/pyrebox

9. Fail2Ban
• Fail2ban scans log files (e.g. /var/log/apache/error_log) and bans IPs that show the malicious signs too many password failures, seeking for exploits, etc. Generally, Fail2Ban is then used to update firewall rules to reject the IP addresses for a specified amount of time, although any arbitrary other action (e.g. sending an email) could also be configured. Out of the box Fail2Ban comes with filters for various services (apache, courier, ssh, etc).
• Fail2Ban can reduce the rate of incorrect authentications attempts however it cannot eliminate the risk that weak authentication presents. Configure services to use only two factor or public/private authentication mechanisms if you really want to protect services.

https://www.fail2ban.org/wiki/index.php/Main_Page

10. OSSEC
• OSSEC is a full platform to monitor and control your systems. It mixes all the aspects of HIDS (host-based intrusion detection), log monitoring and SIM/SIEM together in a simple, powerful and open-source solution.

https://github.com/ossec/ossec-hids
https://www.ossec.net/

11. RKHunter and CHRookit

https://rkhunter.sourceforge.net/
http://chkrootkit.org/

12. Process Hacker
• A free powerful multi-purpose tool that helps you monitor system resources, debug software and detect malware.

https://processhacker.sourceforge.io/downloads.php

13. Splunk
• Its software helps capture, index and correlate real-time data in a searchable repository, from which it can generate graphs, reports, alerts, dashboards and visualizations. Splunk uses machine data for identifying data patterns, providing metrics, diagnosing problems and providing intelligence

for business operations. Splunk is a horizontal technology used for application management, security and compliance, as well as business and web analytics.

https://www.splunk.com/

14. Wazuh
• Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance.

https://wazuh.com/

15. TheHive

• A scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.

https://thehive-project.org/

16. Security Onion
• Our products include both the Security Onion software and specialized hardware appliances that are built and tested to run Security Onion. Our appliances will save you and your team time and resources, allowing you to focus on keeping your organization secure.

https://securityonionsolutions.com/

17. Caine
• CAINE (Computer Aided INvestigative Environment) is an Italian GNU/Linux live distribution created as a Digital Forensics project

https://www.caine-live.net/

18. CALDERA
What does CALDERA do?
• CALDERA helps cybersecurity professionals reduce the amount of time and resources needed for routine cybersecurity testing.
• CALDERA empowers cyber teams in three main ways:
Autonomous Adversary Emulation
• With CALDERA, your cyber team can build a specific threat (adversary) profile and launch it in a network to see where you may be susceptible. This helps with testing defences and training blue teams on how to detect specific threats.
Autonomous Incident Response
• Enables your team to perform automated incident response on a given host, allowing them to find new ways to identify and respond to threats.
Manual Red-Team Engagements

• Helps your red team perform manual assessments with computer assistance by augmenting existing offensive toolsets. The framework can be extended with any custom tools you may have.

https://caldera.mitre.org/

19. Atomic Red Team

https://atomicredteam.io/

20. Metta
• Metta is an information security preparedness tool. This project uses Redis/Celery, python, and vagrant with virtual box to do adversarial simulation. This allows you to test (mostly) your host-based instrumentation but may also allow you to test any network-based detection and controls depending on how you set up your vagrants. The project parses yaml files with actions and uses celery to queue these actions up and run them one at a time without interaction.

https://github.com/uber-common/metta

21. OSSIM
• AlienVault® OSSIM™, Open-Source Security Information and Event Management (SIEM), provides you with a feature-rich open source SIEM complete with event collection, normalization and correlation. Launched by security engineers because of the lack of available open-source products, AlienVault OSSIM was created specifically to address the reality many securities professionals face: A SIEM, whether it is open source or commercial, is virtually useless without the basic security controls necessary for security visibility.

https://cybersecurity.att.com/products/ossim

22. Prelude
• Prelude is a Universal "Security Information & Event Management" (SIEM) system. Prelude collects, normalizes, sorts, aggregates, correlates and reports all security-related events independently of the product brand or license giving rise to such events; Prelude is "agentless".
• As well as being capable of recovering any type of log (system logs, syslog, flat files, etc.), Prelude benefits from a native support with several systems dedicated to enriching information even further (snort, samhain, ossec, auditd, etc.).

https://www.prelude-siem.org/

23. Nagios
• Nagios XI provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party addons provide for monitoring of virtually all in-house and external applications, services, and systems.

https://www.nagios.org/

24. Zabbix

25. Icinga
• Find answers, take actions and become a problem-solver. Be flexible and take your own ways. Stay curious, stay passionate, stay in the loop. Tackle your monitoring challenge.

https://icinga.com/

26. Helk
• The Hunting ELK or simply the HELK is one of the first open-source hunt platforms with advanced analytics capabilities such as SQL declarative language, graphing, structured streaming, and even machine learning via Jupyter notebooks and Apache Spark over an ELK stack. This project was developed primarily for research, but due to its flexible design and core components, it can be deployed in larger environments with the right configurations and scalable infrastructure.

https://github.com/Cyb3rWard0g/HELK

27. CimSweep
• CimSweep is a suite of CIM/WMI-based tools that enable the ability to perform incident response and hunting operations remotely across all versions of Windows. CimSweep may also be used to engage in offensive reconnaissance without the need to drop any payload to disk. Windows Management Instrumentation has been installed and its respective service running by default since Windows XP and Windows 2000 and is fully supported in the latest versions of Windows including Windows 10, Nano Server, and Server 2016.

https://github.com/PowerShellMafia/CimSweep

28. PowerForensics
• The purpose of PowerForensics is to provide an all-inclusive framework for hard drive forensic analysis. PowerForensics currently supports NTFS and FAT file systems, and work has begun on Extended File System and HFS+ support.

https://github.com/Invoke-IR/PowerForensics

29. RedLine
• Redline®, FireEye's premier free endpoint security tool, provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis and the development of a threat assessment profile.
With Redline, you can:
• Thoroughly audit and collect all running processes and drivers from memory, file-system metadata, registry data, event logs, network information, services, tasks and web history.
• Analyse and view imported audit data, including the ability to filter results around a given timeframe using
• Redline's Timeline functionality with the TimeWrinkle™ and TimeCrunch™ features.
• Streamline memory analysis with a proven workflow for analysing malware based on relative priority.

• Perform Indicators of Compromise (IOC) analysis. Supplied with a set of IOCs, the Redline Portable Agent is automatically configured to gather the data required to perform the IOC analysis and an IOC hit result review.

https://www.fireeye.com/services/freeware/redline.html

30. Yara
• YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a. rule, consists of a set of strings and a boolean expression which determine its logic.

https://github.com/VirusTotal/yara

31. Forager
• Do you ever wonder if there is an easier way to retrieve, store, and maintain all your threat intelligence data? Random user, meet Forager. Not all threat intel implementations require a database that is "correlating trillions of data points." and instead, you just need a simple interface, with simple TXT files, that can pull threat data from other feeds, PDF threat reports, or other data sources, with minimal effort. With 15 pre-configured threat feeds, you can get started with threat intelligence feed management today

https://github.com/opensourcesec/Forager

32. Threat Bus
• Connect Open-Source Security Tools: Threat Bus is a pub-sub broker for threat intelligence data. With Threat Bus you can seamlessly integrate threat intel platforms like OpenCTI or MISP with detection tools and databases like Zeek or VAST.
• Native STIX-2: Threat Bus transports indicators and sightings encoded as per the STIX-2 open format specification.
• Plugin-based Architecture: The project is plugin-based and can be extended easily. Read about the different plugin types and how to write your own. We welcome contributions to adopt new open-source tools!
• Official Plugins: We maintain many plugins right in the official Threat Bus repository. Check out our integrations for MISP, Zeek, CIFv3, and generally apps that connect via ZeroMQ, like vast-threatbus and our OpenCTI connector.
• Snapshotting: The snapshot feature allows subscribers to directly request threat intelligence data for a certain time range from other applications. Threat Bus handles the point-to-point communication of all involved apps.

https://github.com/tenzir/

33. ThreatIngestor
• ThreatIngestor can be configured to watch Twitter, RSS feeds, or other sources, extract meaningful information such as malicious IPs/domains and YARA signatures, and send that information to another system for analysis.

34. MISP
• User guide for MISP - The Open Source Threat Intelligence Sharing Platform. This user guide is intended for ICT professionals such as security analysts, security incident handlers, or malware reverse engineers who share threat intelligence using MISP or integrate MISP into other security monitoring tools. The user guide includes day-to-day usage of the MISP's graphical user interface along with its automated interfaces (API), to integrate MISP within a security environment and operate one or more MISP instances.

35. Malware-IOC
• Here are indicators of compromise (IOCs) of our various investigations. We are doing this to help the broader security community fight malware wherever it might be
• .yar files are Yara rules
• .rules files are Snort rules
• S\samples.md5, samples.sha1 and samples.sha256 files are newline separated list of hexadecimal digests of malware samples
• If you would like to contribute improved versions, please send us a pull request.
• If you've found false positives give us the details in an issue report and we'll try to improve our IOCs.
• These are licensed under the permissive BSD two-clause license. You are allowed to modify these and keep the changes to yourself even though it would be rude to do so.

36. Cobalt Strike Scan
• Scan files or process memory for Cobalt Strike beacons and parse their configuration.
• CobaltStrikeScan scans Windows process memory for evidence of DLL injection (classic or reflective injection) and/or performs a YARA scan on the target process' memory for Cobalt Strike v3 and v4 beacon signatures.
• Alternatively, CobaltStrikeScan can perform the same YARA scan on a file supplied by absolute or relative path as a command-line argument.
• If a Cobalt Strike beacon is detected in the file or process, the beacon's configuration will be parsed and displayed to the console.

37. Hardentools
• Hardentools is designed to disable several "features" exposed by operating systems (Microsoft Windows, for now) and some widely used applications (Microsoft Office and Adobe PDF Reader, for now). These features, commonly thought for enterprise customers, are generally useless to regular users and rather pose as dangers as they are very commonly abused by attackers to execute malicious code on a victim's computer. The intent of this tool is to simply reduce the attack surface by disabling the low-hanging fruit. Hardentools is intended for individuals at risk, who might want an extra level of security at the price of some usability. It is not intended for corporate environments.

38. Windows Secure Host Baseline

• The Windows Secure Host Baseline (SHB) provides an automated and flexible approach for assisting the DoD in deploying the latest releases of Windows 10 using a framework that can be consumed by organizations of all sizes.

• The DoD CIO issued a memo on November 20, 2015, directing Combatant Commands, Services, Agencies and Field Activities (CC/S/As) to rapidly deploy the Windows 10 operating system throughout their respective organizations with the objective of completing deployment by the end of January 2017. The Deputy Secretary of Defence issued a memo on February 26, 2016, directing the DoD to complete a rapid deployment and transition to Microsoft Windows 10 Secure Host Baseline by the end of January 2017.

https://github.com/nsacyber/Windows-Secure-Host-Baseline

39. Any Run

• It is not enough to run a suspicious file on a testing system to be sure in its safety. For some types of malware or vulnerabilities (e.g., APT), direct human interaction during analysis is required. A set of online malware analysis tools, allows you to watch the research process and make adjustments when needed, just as you would do it on a real system, rather than relying on a wholly automated sandbox.

https://any.run/

40. Hybrid Analysis

• This is a free malware analysis service for the community that detects and analyses unknown threats using a unique Hybrid Analysis technology.

https://www.hybrid-analysis.com/

41. PSHunt

• PSHunt is a Powershell Threat Hunting Module designed to scan remote endpoints* for indicators of compromise or survey them for more comprehensive information related to state of those systems (active processes, autostarts, configurations, and/or logs).

• PSHunt began as the precurser to Infocyte's commercial product, Infocyte HUNT, and is now being open sourced for the benefit of the DFIR community.

https://github.com/Infocyte/PSHunt

42. GoPhish

• Gophish is a powerful, open-source phishing framework that make it easy to test your organization's exposure to phishing.

https://getgophish.com/

43. Solar Winds

• The log manager gathers log messages from all over your system, consolidating the different formats they are written in to be stored and searched together. The dashboard shows all events live on the screen, and there is also an analytical tool that helps you search through stored log files for pertinent security information. The log manager also protects logfiles from tampering with a file integrity monitor.
• The Security Event Manager isn't just a SIEM. It includes a threat intelligence feed, which pools threat detection experiences from all the clients of the SolarWinds system. The security system uses the guidance from the feed when searching through log messages for indicators of attack.

https://www.solarwinds.com/security-event-manager

44. SentinelOne
• Today we are pleased to announce the revolutionary technology of ActiveEDR. ActiveEDR solves the problems of EDR as you know it by tracking and contextualizing everything on a device. ActiveEDR is able to identify malicious acts in real time, automating the required responses and allowing easy threat hunting by searching on a single IOC. Read more to understand how we got here and how we created the first and only EDR that is truly active.

https://www.sentinelone.com/blog/active-edr-feature-spotlight/

45. Qualys
• Cyber risk is business risk - with risks growing faster than what traditional VM and SIEM tools can manage. Security and IT teams need a new approach to tackle cyber threats with a clear understanding of cybersecurity risk and automate workflows for rapid response

https://www.qualys.com/apps/vulnerability-management-detection- response/

46. EzTools
• These open-source digital forensics tools can be used in a wide variety of investigations including cross validation of tools, providing insight into technical details not exposed by other tools, and more. Over the years, Eric has written and continually improve over a dozen digital forensics tools that investigators all over the world use and rely upon daily.

https://www.sans.org/tools/ez-tools/

47. REMnux
• REMnux® is a free Linux toolkit for assisting malware analysts with reverse- engineering malicious software. It strives to make it easier for forensic investigators and incident responders to start using the variety of freely available tools that can examine malware yet might be difficult to locate or set up.
• The heart of the project is the REMnux Linux distribution based on Ubuntu. This lightweight distro incorporates many tools for analysing Windows and Linux malware, examining browser-based threats such as obfuscated JavaScript, exploring suspicious document files and taking apart other malicious artifacts. Investigators can also use the distro to intercept suspicious network traffic in an isolated lab when performing behavioural malware analysis.

https://sansgear.com/remnux/

48. Sift Workstation
• Why SIFT? The SIFT Workstation is a group of free open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite. SIFT demonstrates that advanced incident response capabilities and deep dive digital forensic techniques to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

https://sansgear.com/sift-workstation/

49. Sof-Elk
• SOF-ELK® is a "big data analytics" platform focused on the typical needs of computer forensic investigators/analysts and information security operations personnel. The platform is a customized build of the open source Elastic stack, consisting of the Elasticsearch storage and search engine, Logstash ingest and enrichment system, Kibana dashboard frontend, and Elastic Beats log shipper (specifically filebeat). With a significant amount of customization and ongoing development, SOF-ELK® users can avoid the typically long and involved setup process the Elastic stack requires. Instead, they can simply download the pre-built and ready-to-use SOF- ELK® virtual appliance that consumes various source data types (numerous log types as well as NetFlow), parsing out the most critical data and visualizing it on several stock dashboards. Advanced users can build visualizations the suit their own investigative or operational requirements, optionally contributing those back to the primary code repository.

https://sansgear.com/sof-elk/

50. MXToolbox
• This test will list MX records for a domain in priority order. The MX lookup is done directly against the domain's authoritative name server, so changes to MX Records should show up instantly. You can click Diagnostics, which will connect to the mail server, verify reverse DNS records, perform a simple Open Relay check and measure response time performance. You may also check each MX record (IP Address) against 105 DNS based blacklists. (Commonly called RBLs, DNSBLs)

https://mxtoolbox.com/

51. DevSec.io
• Server hardening framework providing Ansible, Chef, and Puppet implementations of various baseline security configurations.

https://dev-sec.io/

52. Clevis
• Pluggable framework for automated decryption, often used as a Tang client.

https://github.com/latchset/clevis

53. Cortex
• Provides horizontally scalable, highly available, multi-tenant, long term storage for Prometheus.

https://cortexmetrics.io/

54. Jaeger
• Distributed tracing platform backend used for monitoring and troubleshooting microservices-based distributed systems.

https://www.jaegertracing.io/

55. KubeSec
• Static analyser of Kubernetes manifests that can be run locally, as Kubernetes admission controller, or as its own cloud service.

https://kubesec.io/

56. Linkerd
• Ultra-light Kubernetes-specific service mesh that adds observability, reliability, and security to Kubernetes applications without requiring any modification of the application itself.

https://linkerd.io/

57. Globaleaks
• Free, open-source software enabling anyone to easily set up and maintain a secure whistleblowing platform.

https://www.globaleaks.org/

58. Teleport
• Allows engineers and security professionals to unify access for SSH servers, Kubernetes clusters, web applications, and databases across all environments.

https://goteleport.com/

59. DynInst
• Tools for binary instrumentation, analysis, and modification, useful for binary patching.

https://dyninst.org/dyninst

60. Dynamo Rio
• Runtime code manipulation system that supports code transformations on any part of a program, while it executes, implemented as a process-level virtual machine.

https://dynamorio.org/

61. Egalito

• Binaries recompile and instrumentation framework that can fully disassemble, transform, and regenerate ordinary Linux binaries designed for binary hardening and security research.

https://egalito.org/

62. Kushtaka
• Sustainable all-in-one honeypot and honeytoken orchestrator for under-resourced blue teams.

https://kushtaka.org/

63. Manuka
• Open-sources intelligence (OSINT) honeypot that monitors reconnaissance attempts by threat actors and generates actionable intelligence for Blue Teamers.

https://github.com/spaceraccoon/manuka

64. Threat Note
• Web application built by Defense Point Security to allow security researchers the ability to add and retrieve indicators related to their research.

https://github.com/DefensePointSecurity/threat_note

65. AutoMacTC
• Modular, automated forensic triage collection framework designed to access various forensic artifacts on macOS, parse them, and present them in formats viable for analysis.

https://github.com/CrowdStrike/automactc

66. Margarita Shotgun
• Command line utility (that works with or without Amazon EC2 instances) to parallelize remote memory acquisition.

https://github.com/ThreatResponse/margaritashotgun

67. Mailspoof
• Scans SPF and DMARC records for issues that could allow email spoofing.

https://github.com/serain/mailspoof

68. Phishing Catcher
• Configurable script to watch for issuances of suspicious TLS certificates by domain name in the Certificate Transparency Log (CTL) using the CertStream service.

https://github.com/x0rz/phishing_catcher

69. BadBlood

• Fills a test (non-production) Windows Domain with data that enables security analysts and engineers to practice using tools to gain an understanding and prescribe to securing Active Directory.

https://www.secframe.com/badblood/

70. Drool
• Replay DNS traffic from packet capture files and send it to a specified server, such as for simulating DDoS attacks on the DNS and measuring normal DNS querying.

https://www.dns-oarc.net/tools/drool

71. Dumpster Fire
• Modular, menu-driven, cross-platform tool for building repeatable, time-delayed, distributed security events for Blue Team drills and sensor/alert mapping.

https://github.com/TryCatchHCF/DumpsterFire

72. GRR Rapid Response
• Incident response framework focused on remote live forensics consisting of a Python agent installed on assets and Python-based server infrastructure enabling analysts to quickly triage attacks and perform analysis remotely.

https://github.com/google/grr

73. MozDef
• Automate the security incident handling process and facilitate the real-time activities of incident handlers.

https://github.com/mozilla/MozDef

74. Rastrea2r
• Multi-platform tool for triaging suspected IOCs on many endpoints simultaneously and that integrates with antivirus consoles.

https://github.com/rastrea2r/rastrea2r

75. AttackerKB
• Free and public crowdsourced vulnerability assessment platform to help prioritize high-risk patch application and combat vulnerability fatigue.

https://attackerkb.com/

76. DATA
• Credentials phish analysis and automation tool that can accept suspected phishing URLs directly or trigger on observed network traffic containing such a URL.

https://github.com/hadojae/DATA

77. Unfetter
• Identifies defensive gaps in security posture by leveraging Mitre's ATT&CK framework.

https://nsacyber.github.io/unfetter/

78. Onion Balance
• Provides load-balancing while also making Onion services more resilient and reliable by eliminating single points-of-failure.

https://onionbalance.readthedocs.io/en/latest/

79. Nebula
• Completely open source and self-hosted, scalable overlay networking tool with a focus on performance, simplicity, and security, inspired by tinc.

https://github.com/slackhq/nebula

80. TailScale
• Managed freemium mesh VPN service built on top of WireGuard.

https://tailscale.com/

81. Sigcheck
• Audit a Windows host's root certificate store against Microsoft's Certificate Trust List (CTL).

https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck

82. Domain Hunter
• Checks expired domains for categorization/reputation and Archive.org history to determine good candidates for phishing and C2 domain names

https://github.com/threatexpress/domainhunter

83. Elastic for Red Team
• Repository of resources for configuring a Red Team SIEM using Elastic.

https://github.com/SecurityRiskAdvisors/RedTeamSIEM

84. SharpEDRChecker
• Checks running processes, process metadata, Dlls loaded into your current process and each DLLs metadata, common install directories, installed services and each service binaries metadata, installed drivers and each driver's metadata, all for the presence of known defensive products such as AV's, EDR's and logging tools.

https://github.com/PwnDexter/SharpEDRChecker

85. SeatBelt

• Seatbelt is a C# project that performs several security-oriented hosts-survey "safety checks" relevant from both offensive and defensive security perspectives.

https://github.com/GhostPack/Seatbelt

86. BloodHound

• Six Degrees of Domain Admin

https://github.com/BloodHoundAD/BloodHound

87. Rubeus

• Rubeus is a C# toolset for raw Kerberos interaction and abuses. It is heavily adapted from Benjamin Delpy's Kekeo project (CC BY-NC- SA 4.0 license) and Vincent LE TOUX's MakeMeEnterpriseAdmin project (GPL v3.0 license).

https://github.com/GhostPack/Rubeus

88. Mimikatz

• Mimikatz is an open-source application that allows users to view and save authentication credentials like Kerberos tickets.

https://github.com/gentilkiwi/mimikatz

89. CredBandit

• CredBandit is a proof-of-concept Beacon Object File (BOF) that uses static x64 syscalls to perform a complete in memory dump of a process and send that back through your already existing Beacon communication channel.

https://github.com/xforcered/CredBandit

90. SharpChromium

• .NET 4.0 CLR Project to retrieve Chromium data, such as cookies, history and saved logins.

https://github.com/djhohnstein/SharpChromium

91. Watson

• Watson is a .NET tool designed to enumerate missing KBs and suggest exploits for Privilege Escalation vulnerabilities.

https://github.com/rasta-mouse/Watson

92. DNS Exfiltration

• Data exfiltration over DNS request covert channel

https://www.sentinelone.com/blog/active-edr-feature-spotlight/

93. Prelude Operator
• A Platform for Developer-first advanced security· Defend your organization by mimicking real adversarial attacks.

https://www.prelude.org/

94. Stratus Red Team
• Stratus Red Team is "Atomic Red Team™" for the cloud, allowing to emulate offensive attack techniques in a granular and self-contained manner.

https://github.com/DataDog/stratus-red-team

95. FastFinder
• Fast customisable cross-platform suspicious file finder. Supports md5/sha1/sha256 hashes, literal/wildcard strings, regular expressions and YARA rules.

https://github.com/codeyourweb/fastfinder

96. Fireeye Memorize
• A free memory forensic software.

https://fireeye.market/apps/211368

97. KeeFarce
• Extract KeePass passwords from memory.

https://github.com/denandz/KeeFarce

98. Logon Tracer
• Investigate malicious Windows logon by visualizing and analysing Windows event log

https://github.com/JPCERTCC/LogonTracer

99. RegRippy
• A framework for reading and extracting useful forensics data from Windows registry hives

https://github.com/airbus-cert/regrippy

100.   Pancake Viewer
• Disk image viewer based in dfvfs, like the FTK Imager viewer

https://github.com/forensicmatt/PancakeViewer